CUSTOMER NO.: 24498
Ser. No. 10/030,766
Office Action dated: 01/11/07
Response dated: 07/02/07

PATENT
RCA 89,520

Remarks/Arguments

Claims 1-7 and 9-10 are pending. The claims have been amended to more clearly and distinctly claim the subject matter that Applicants regard as their invention. No new matter is believed to be added by the present amendment.

Rejection of claims 1-7 and 9-10 under 35 USC 103(a) as being unpatentable over Kaganas et al. (US 6425018), Tanaka et al. (US 6446177) and Truong et al. (US Pat No 6173057)

Applicants submit that for at least the reasons discussed below the present amended claims are patentably distinguishable over the cited combination of references.

Amended claim 1 recites:

> "determining a unique identification associated with the removable data storage device coupled to the handheld audio playback device, and **decrypting the audio data file using the unique identification** and decrypting the associated decoder file using a first key;
>
> 'decoding the decrypted audio data file in accordance with the decrypted decoder file in the digital signal processor,".

Applicants submit that none of the references, singly or in combination, disclose or suggest at least the above-emphasized limitation of amended claim 1.

The office action acknowledges that Kaganas fails to teach the step of decrypting the audio data file using a unique identification associated with the storage device and decrypting the decoder file using a first key. Tanaka is cited as teaching a system for protecting literary works on a flash card with encryption based on a unique identification associated with the storage device. However, the Office Action acknowledges that the combination of references still fails to teach or suggest , "... the encryption method of the associated codes's, decoder files, or programs, which is found on a memory card in the system taught by Kaganas."

Truong is cited to provide the missing element. In particular, Truong is cited as teaching the feature, "...decrypting the audio data file using the unique

identification and decrypting the associated decoder file using a first key', wherein the unique identification, as taught by Tanaka, is a CIS value, or the like, taken from the recording medium to create an encrypted signature... (OA page 4, lines 11-14)"

For the reasons discussed in Applicants' previous responses, Applicants respectfully submit that Truong fails to teach or suggest the limitation "... decrypting the audio data file using the unique identification ..."

In review, Truong teaches a system that uses a **separate recording medium** having information stored thereon, **and a portable medium** (e.g. smart card) having security information stored thereon for enabling a user to access the information on the recording medium using a computer platform (col. 4, lines 5-14). The recording medium is a non-rewritable medium, wherein the contents of the medium can be read but not modified or altered (col. 3, lines 8-10).

The recording medium may include an identity parameter specific to the medium to secure the recording medium (col. 3, lines 22-24). However, the identity parameter associated with the recording medium is not associated at all with a step of decrypting data files stored on the recording medium. Rather, the identity parameter is used by the hardware security device to **confirm the identity of the recording medium** during the first step of the process for accessing data on the medium (col. 4, lines 24-37). Once the identity of the recording medium has been confirmed, various steps are performed to authenticate the integrity of the software on the recording medium using various signatures stored on the recording medium (col. 4, lines 38-44). Then, various security checks are performed to ensure proper security levels and that there have been no breaches of the method (col. 4, line 59 - col. 5, line 22). Nowhere does Truong teach or suggest that the identity parameter of the recording medium is used to decrypt the data files stored on the recording medium.

The portions of Truong cited by the Office Action fail to teach or suggest the above cited limitation of claim 1. The examiner alleges that col. 4, line 24-58 of Truong teaches that "the decoding utilizes the unique identification specific to the recording medium to decode the data." In fact, the cited portion of Truong describes the first two steps in the process for enabling user access to the

encrypted information on the recording medium, wherein the security hardware device and the associated software identify the recording medium and verify the integrity of the content on the medium.

In the first step, the identity of the recording medium is verified. See for example, col. 4, lines 25-26 "First, the hardware security device and the associated software identify the recording medium." In this step, the identify parameter of the recording medium is compared with the identity parameter prerecorded in the hardware security device (col. 4, lines 26-34). However, the verification of the identity **does not enable user access** to the information on the recording medium (see col. 4, lines 35-37, "Successful identification of the recording medium does not give the user access to the information stored on the medium.")

The second step involves verifying the integrity of the information stored on the recording medium (col. 4, lines 38-40). In this step, the encrypted signature stored on the recording medium is compared with a signature stored on the hardware security device (col. 4, lines 40-43). The comparison of the signatures allows the security device to determine whether content stored on the recording medium has been modified (col. 4, lines 46-49). However, this second step is directed to verifying a **particular condition** of the content stored on the recording medium and **does not provide access** to the content. Certainly, nowhere does the cited portion teach or suggest that the decoding utilizes the unique identification specific to the recording medium to decode the data as alleged by the Office Action.

The Office Action further alleges that, "the unique encrypted signature is based on information on the recorded medium (Col. 4, lines 44-45) and the keys associated with decrypting the associated data and programs are also based on values found in the security table (col. 3, lines 25-26 and lines 34-36)."

Regarding the first citation, Truong states "The calculation of the signature is based on information taken from the recording medium." Here, "signature" refers to the encrypted signature that is compared with the signature stored on the security hardware during the second step to verify the integrity of the content stored on the recording medium. It does not relate to a key used to decrypt the content on the recording medium.

Regarding second citation, Truong actually states "... and a security table containing decoding algorithms in encrypted form" and "Some or all of the information is encoded or encrypted to provide better protection in accordance with the above-mentioned security table." These portions simply refer to the fact that the security table includes decoding algorithms, which are stored in encrypted form. However, nowhere do these citations mention or suggest that the **data** stored on the recording medium is decrypted using keys stored in the security table as alleged by the Office Action.

In fact, as previously discussed by Applicants, Truong specifically teaches that the information necessary for accessing the content stored on the recording medium is derived from a separate memory card. See for example:

> The publisher supplies the user a recording medium and a portable medium (e.g., smart card). The publisher may record the following information on the smart card: An identity code specific to the user (i.e., a PIN code); **Keys for decoding or decrypting information stored on the recording medium** ... (col. 4, lines 5-10, emphasis added)

See also:

> Thus, in order to implement the present invention, the user's computer platform must be properly secured, and the user must have available not only the recording medium containing at least the data and/or applications and accompanying operating software, but **must** also have available **a memory card defining, in particular, conditions for accessing the recording medium** (col. 6, lines 12-18, emphasis added)

Thus, Truong requires that information for accessing the content on the recording medium must be provided on a separate medium. This is completely contrary to the limitation recited in the present claims that the audio data file is decrypted using the unique identification associated with the removable data storage device. The Office Action states that it is implied that the security table includes keys that are used to encode/decode the various **data** and/or applications. However, as seen by the citations above, Truong specifically teaches away from such an implication, and explicitly states that the keys for decrypting the

content on the recording medium are stored on a **separate** memory card or smart card.

In view of the above, Applicants submit that even if it is proper to combine the cited references in the manner suggested by the Office Action, the combined references still fail to disclose or suggest each and every limitation of the present claims. Therefore, Applicants respectfully submit that claims 1, 4, 6 and 10, and the claims that depend therefrom, are patentably distinguishable over the suggested combination of references.

Having fully addressed the Examiner's rejections it is believed that, in view of the preceding amendments and remarks, this application stands in condition for allowance. Accordingly then, reconsideration and allowance are respectfully solicited. If, however, the Examiner is of the opinion that such action cannot be taken, the Examiner is invited to contact the Applicants' attorney at (609) 734-6815, so that a mutually convenient date and time for a telephonic interview may be scheduled.

Respectfully submitted,
SIN HUI CHEAH ET AL.

By: _____
Paul P. Kiel
Attorney for Applicants
Registration No. 40,677

PPK:pdf

THOMSON Licensing LLC
Patent Operations
P.O. Box 5312
Princeton, NJ 08543-5312

July 2, 2007